UNITED STATES DISTRICT COURT
DISTRICT OF CONNECTICUT

UNITED STATES OF AMERICA, *Plaintiff,* v. AHMAD KHALIL ELSHAZLY, *Defendant.*	: : : : : : : : : :	No: 3:20-CR-00071(VAB)

PROTECTIVE ORDER
PERTAINING TO CLASSIFIED INFORMATION

This matter comes before the Court upon the motion of the United States for a Protective Order Regarding Classified Information to prevent the unauthorized disclosure or dissemination of classified national security information and documents that may be reviewed by or made available to the defendant's counsel by the government during the prosecution of this case. Pursuant to the authority granted under Section 3 of the Classified Information Procedures Act, 18 U.S.C. App. 3 (2000) ("CIPA"), the Security Procedures Established Pursuant to CIPA by the Chief Justice of the United States for the Protection of Classified Information (reprinted following CIPA section (9)), Rules 16(d) and 57 of the Federal Rules of Criminal Procedure, and the general supervisory authority of the Court, and in order to protect the national security, the following Protective Order is entered.

The Court finds this case will involve information that has been classified in the interest of national security of the United States pursuant to Executive Order 13526, as amended. The storage, handling and control of this information will require special security precautions mandated by statute, executive order, and regulation, and access to which requires the appropriate security clearances, and a "need to know" determination pursuant to Executive Order 13526.

The purpose of this Protective Order is to establish procedures that must be followed by the Defense and the Government, and any other person who receives access to, or otherwise is in possession of, classified information as a result of their participation in this case. These procedures will apply to all pretrial, trial, post-trial, and appellate matters concerning classified information, and may be modified from time to time by further order of the Court pursuant to Rule 16(d) of the Federal Rules of Criminal Procedure, CIPA Section 3, and the Court's inherent supervisory authority.

Definitions

The following definitions shall apply to this Order:

1. The term "classified information" shall mean:

a. Any document or information contained therein, which has been classified by any Executive Branch agency in the interests of national security pursuant to Executive Order 13526, as amended, or its predecessor orders, as "CONFIDENTIAL", "SECRET", "TOP SECRET", or additionally controlled as "SENSITIVE COMPARTMENTED INFORMATION" ("SCI");

b. Any document or information that is currently properly classified, as set forth in (a), and that has been approved by the Government or the Court for release to one or more of the defendant's counsel;

c. Any document or information, regardless of its physical form or characteristics now or formerly in the possession of a private party which (1) has been derived from information from the United States Government that was classified, and (2) has subsequently been classified by the United States pursuant to executive order as "CONFIDENTIAL", "SECRET", "TOP SECRET", or additionally controlled as SCI;

d. "Foreign government information," as that term is defined in Executive Order 12958, as amended by Executive Order 13292;

e. Verbal classified information known to the defendant or defense counsel; and

f. Any document or information the Defense knows or reasonably should know contains classified information, including information acquired or conveyed orally;

2. The terms "document," "materials," and "information" shall include, but are not limited to:

a. All written, printed, visual or audible matter of any kind, formal or informal, including originals, conforming copies, and non-conforming copies (whether different from the original by reason of notation made on such copies or otherwise);

b. Notes (handwritten, oral, or electronic); papers; letters; correspondence; memoranda; reports; summaries; photographs; maps; charts; graphs; inter-office communications; notations of any sort concerning conversations, meetings or other communications; bulletins; teletypes; telecopies; telegrams; telexes; transcripts; cables; facsimiles; invoices; worksheets; drafts; microfiche; microfilm; videotapes; sound recordings of any kind; motion pictures; electronic, mechanical or electric records of any kind, including but not limited to tapes, cassettes, disks, recordings, films, typewriter ribbons, word processing or other computer tapes, disks, or thumb drives and all manner of electronic data processing storage; and as well as alterations, amendments, modifications, and changes of any kind to the foregoing and all recordings of information on magnetic, electronic, or optical media (including but not limited to those on CD-ROM), typewriter ribbons, films and all manner of electronic data processing storage; and

c. Information obtained orally.

3. The term "access to classified information" shall mean having access to, reviewing, reading, learning, or otherwise coming to know in any manner classified information.

4. The term "Secure Area" shall mean a facility approved by a Classified Information Security Officer ("CISO") for the review, storage, handling and control of classified information.

5. "Need-to-know" means a determination within the executive branch in accordance with directives issued pursuant to this order that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function.

Classified Information: General Provisions

All classified documents, and information contained therein, shall remain classified unless the documents bear a clear indication that they have been declassified by the agency or department that originated the document or information contained therein (the "originating agency").

Any classified information provided to defense counsel by the Government is to be used solely by defense counsel and solely for the purpose of litigating this case. Defense counsel may not disclose or cause to be disclosed in connection with this case any information known or reasonably believed to be classified information except as otherwise provided herein.

Defense counsel may not confirm or deny to any defendant assertions made by any defendant based on knowledge defense counsel may have obtained from classified information, except where that classified information has been provided to the defendant pursuant to this Order.

Defense counsel shall not disclose classified information to any person, except to the Court, Government personnel who hold appropriate security clearances and have been determined to have a need to know that information, and those authorized pursuant to this Order.

Information that is classified that also appears in the public domain is not thereby automatically declassified unless it appears in the public domain as the result of an official statement by a U.S. Government Executive Branch official who is authorized to declassify the information. Individuals who by virtue of this Order or any other court order are granted access to classified information may not confirm or deny classified information that appears in the public domain. Prior to any attempt by defense counsel to have such information confirmed or denied at any public proceeding in these appeals, defense counsel must comply with the notification requirements of Section 5 of CIPA and all provisions of this Order.

In the event that classified information enters the public domain, defense counsel is precluded from making private or public statements where the statements would reveal personal knowledge from non-public sources regarding the classified status of the information, or would disclose that defense counsel had personal access to classified information confirming, contradicting, or otherwise relating to the information already in the public domain. Defense counsel is not precluded from citing or repeating information in the public domain that counsel does not know or have reason to believe to be classified information, or derived from classified information.

Security Procedures

In accordance with the provisions of the Classified Information Procedures Act ("CIPA") and the security procedures promulgated by the Chief Justice of the United States pursuant to that Act, this Court has designated Harry J. Rucker as the Classified Information Security Officer ("CISO") for this case for the purpose of providing security arrangements necessary to protect any classified information or documents that will be made available to the defense in connection with this case. This Court also designated Daniel O. Hartenstine, Matthew W. Mullery, Maura L.

Peterson, Carli V. Rodriguez-Feo, and W. Scooter Slade as alternate CISOs for this case, for the purpose of providing security arrangements necessary to protect against unauthorized disclosure any classified information that has been made available to defense counsel in connection with this case. Defense counsel shall seek guidance from the CISO with regard to appropriate storage, handling, transmittal, and use of classified information.

The Court has been advised, through the CISO, that the assigned Assistant United States Attorney and trial attorneys for the United States Department of Justice have the requisite security clearances allowing them to have access to the classified information that relates to this case. Any government attorneys who may in the future participate in the litigation of any part of this matter (or supervise such litigation) will have security clearances appropriate for the level of classification of any documents reviewed.

The Court has been advised by the government that James P. Maguire, the Defendant's counsel, has the requisite security clearance allowing him to have access to certain Classified Information that relates to this case. Accordingly, James P. Maguire shall be permitted access to certain Classified Information that may be disclosed or produced by the United States or otherwise is necessary to prepare for proceedings in this case, in accordance with the terms of this Protective Order and any other orders of the Court. Any additional person whose assistance the defense reasonably requires may only have access to classified information in this case after first (a) obtaining permission from this Court, with prior notice to the government; (b) obtaining security clearances through the CISO for access to the required level of classification on a need-to-know basis; and (c) signing the Memorandum of Understanding in the form attached hereto, thereby agreeing to comply with the terms of this Order. The signed Memorandum of Understanding shall be filed with the Court. The substitution, departure, or removal from this case of defense counsel

or any other cleared person associated with the defense as an employee or witness or otherwise, shall not release that person from the provisions of this Order or the Memorandum of Understanding executed in connection with this Order.

***Secure Area for the Defense*:** The CISO shall arrange for and maintain an appropriately approved secure area for the use of defense counsel. The CISO shall establish procedures to assure that the secure area is accessible to defense counsel during business hours and at other times upon reasonable request as approved by the CISO, in consultation with the United States Marshals Service, and in a manner consistent with all restrictions related to the COVID-19 pandemic. The secure area shall contain a separate working area for defense counsel and will be outfitted with any secure office equipment requested by the defense that is reasonable and necessary to the preparation of the defense. The CISO, in consultation with defense counsel, shall establish procedures to assure that the secure area may be maintained and operated in the most efficient manner consistent with the protection of classified information. No classified documents may be removed from the secured area unless so authorized by the CISO with notice provided to the Court. The CISO shall not reveal to the government the content of any conversations he or she may hear among the defense, nor reveal the nature of the documents being reviewed or the work being generated. The presence of the CISO shall not operate to render inapplicable the attorney-client-privilege.

Filing of Papers by the Defense: Any pleading or other document filed by the defense which defense counsel knows, should know, or has reason to believe contain classified information shall be filed under seal with the CISO or his designee and shall be marked "Filed in Camera and Under Seal with the CISO or Designee." The time of physical submission to the CISO or his designee, which shall occur no later than 4:00 p.m. local time, shall be considered the date and

time of filing. The CISO shall promptly examine the pleading or document and, in consultation with representatives of the appropriate agencies, determine whether the pleading or document contains classified information. If the designated classification representative determines the pleading or document contains classified information, the CISO and the designated classification representative shall ensure the relevant portion of the document—and only that portion—is marked with the appropriate classification marking and remains under seal. All portions of all paper filed by the defendant that do not contain classified information shall be immediately unsealed by the CISO and placed in the public record, unless counsel requests that the paper be filed under seal for other reasons. Except in cases where the pleading or document is filed *ex parte*, the CISO shall immediately deliver under seal to the Court and counsel for the United States any pleading or document to be filed by the defendant that contains classified information.

At the time of making a physical submission to the CISO or a designee, counsel shall file on the public record in the CM/ECF system a notice of filing notifying the Court that a submission was made to the CISO. The notice should contain only the case caption and an unclassified title in the filing.

Filing of Papers by the United States: Those portions of pleadings or documents filed by the United States that contain classified information shall be filed under seal with the Court through the CISO. Such pleadings and documents shall be marked, "Filed In Camera and under Seal with the Classified Information Security Officer or Designee." The date and time of physical submission to the CISO or his designee, which shall occur no later than 4:00 p.m. local time, shall be considered the date and time of filing. Unless the paper is filed ex parte, the CISO shall immediately deliver the pleading or document under seal to counsel for the defendant. At the time of making a physical submission to the CISO or a designee, counsel shall file on the public record

in the CM/ECF system a notice of filing notifying the Court that a submission was made to the CISO. The notice should contain only the case caption and an unclassified title in the filing.

Record and Maintenance of Classified Filings*:* The CISO shall maintain a separate sealed record for those materials which are classified. The CISO shall be responsible for maintaining the secured records for purposes of later proceedings or appeal.

Protection of Classified Information**:** The Court finds that the provisions set forth in this order are necessary to protect the classified information involved in this case.

Access to Classified Information by the Defense and Court Personnel:

Pursuant to Section 4 of the security procedures promulgated pursuant to CIPA, no court personnel (except for the District Court Judge) required by this Court for its assistance shall have access to classified information involved in this case unless that person shall first have received the necessary security clearance as determined by the CISO.

Standard Form 86, "Questionnaire for National Security Positions," attached releases, and full fingerprints shall be completed and submitted to the CISO forthwith by all defense counsel not otherwise already cleared, all persons whose assistance the defense reasonably requires, and by such courtroom personnel as the Court requires for its assistance. The CISO shall undertake all reasonable steps to process all security clearance applications in accordance with applicable regulations.

Prior security clearance and a "need to know" as determined by any government entity as applying to one person does not automatically give that person the authority to disclose any classified information to any other individual, even if that individual also has a security clearance. By way of example, but not limitation, defense counsel with appropriate clearances and a need to know, as determined by the Government, are not authorized to discuss or otherwise disclose such

classified information with an uncleared defendant or other counsel absent approval of the Court or written permission of the Government.

The defendant's counsel, and cleared employees of defendant's counsel, additional cleared persons assisting defendant's counsel, and cleared witnesses accompanied by counsel for the defendant (hereinafter, "the defense") shall have access to classified information only as follows:

1. Unless authorized by the CISO, all classified information produced by the government to the defense in discovery or otherwise, and all classified information possessed, created or maintained by the defense, including notes or any other work product, shall be stored, maintained and used only in the secure area established by the CISO. No classified information shall be maintained by the defense in any other place other than the secure area established by the CISO.

2. The defendant's counsel shall have free access to the classified information made available to them in the secure area established by the CISO and shall be allowed to take notes and prepare documents with respect to those materials.

3. No person, including counsel for the defendant, shall copy or reproduce any classified information in any manner or form, except with the approval of the CISO in accordance with the procedures established by the CISO for the operation of the secure area.

4. All documents prepared by the defense (including, without limitation, pleadings or other documents intended for filing with the Court) that defense counsels knows, should know, or have reason to believe contain classified information must be prepared in a secure area on word processing equipment approved by the CISO. All such documents and any associated materials (such as notes, drafts, copies, typewriter ribbons, thumb drives, CDs, DVDs, magnetic recordings, exhibits) that may contain classified information shall be maintained in the secure area unless and

until the CISO determines that those documents or associated materials are unclassified in their entirety. None of these materials shall be disclosed to counsel for the United States.

5. The defense shall discuss classified information only with other cleared persons and only in the secure area or in an area authorized by the CISO.

6. The defense shall not disclose, without prior approval of the Court, the contents of any classified documents or information to any person not named in this Order except the Court, cleared Court personnel, and the attorneys for the United States identified by the CISO as having the appropriate clearances and the need to know. Counsel for the United States shall be given an opportunity to be heard in response to any defense request for disclosure to a person not named in this Order. Any person approved by the Court for disclosure under this paragraph shall be required to obtain the appropriate security clearance, to sign and submit to the Court the Memorandum of Understanding appended to the Order, and to comply with all the terms and conditions of the Order. If preparation of the defense requires that classified information be disclosed to persons not named in this Order, the CISO shall promptly seek to obtain security clearances for them at the request of defense counsel.

7. The defense shall not discuss classified information over any standard commercial telephone instrument or office intercommunication systems, including but not limited to the internet, or in the presence of any person who has not been granted access to classified information by the Court an in accordance with this Order.

8. Any documents written by the defense that defense counsel knows, should know, or has reason to believe might contain classified information shall be transcribed, recorded, typed, duplicated, copied or otherwise prepared only by persons who have received an appropriate approval for access to classified information.

9. Counsel shall not disclose classified information to the defendant absent leave of this Court or written permission of the Government. Counsel for the Government shall be given an opportunity to be heard in response to any Defense request for disclosure to the defendant of such classified information.

Unauthorized Disclosure of Classified Information: Any unauthorized disclosure of classified information may constitute violations of United States criminal laws. In addition, any violation of the terms of this Order shall be brought immediately to the attention of this Court and may result in a charge of contempt of court and possible referral for criminal prosecution. Any breach of this Order may also result in termination of an individual's access to classified information. Persons subject to this Order are advised that direct or indirect unauthorized disclosure, retention, or negligent handling of classified documents or information could cause serious damage, and in some cases, exceptionally grave damage to the national security of the United States or may be used to the advantage of a foreign nation against the interests of the United States. This Protective Order is intended to ensure that those authorized by this Order to receive classified information in connection with this case will never divulge that information to anyone not authorized to receive it, without prior written authorization from the originating agency or an authorized representative of the United States government, or in conformity with this Order, or as required by CIPA.

Conclusion of the Matter: All classified documents and information to which the defense has access in this case are now and will remain the property of the United States. Upon demand of the CISO, the defense shall return to the CISO all classified information in their possession obtained through discovery from the government in this case, or for which they are responsible because of access to classified information. The notes, summaries and other documents prepared

by the defense that defense counsel knows, should know, or has reason to believe contain classified information shall remain at all times in the custody of the CISO until the end of this matter. At the end of this matter, all such notes, summaries and other documents are to be destroyed by the CISO in the presence of defense counsel if so desired. The "end of this matter" is defined as the latest of the following events:

1. Entry of judgment in this case in the District Court, and if there is a conviction, then the completion of any direct appeals (including applications to the United States Supreme Court) or the expiration of the time for same; plus one year or such additional time as may be permitted for post-conviction proceedings;

2. Final resolution (including completion of any court proceedings or appeals, or expiration of the time for same) of any claims relating to this case (such as malpractice, lawyer misconduct or disciplinary claims, or claims of unauthorized disclosure of classified material) which are pending against defense counsel as of the expiration of the time period specified in the preceding paragraph; and

3. Payment of, or other final action on, CJA vouchers submitted by defense counsel and non-lawyers such as interpreters, investigators and experts. Defense counsel or the government may apply to the Court, based on a showing of good cause, for an Order preserving the materials referred to above for a longer period of time.

Notice of this Order: A copy of this Order shall be issued forthwith to the defense counsel who shall be responsible for advising the defendant, any co-counsel, employees of counsel for the defendant, and defense witnesses who need to know of the contents of this Order. Counsel for the defendant and any other individuals who will be provided access to the classified information, shall execute the Memorandum of Understanding described in this Order, and counsel for the

defendant shall file executed originals of such documents with the Court and the CISO and serve an executed original upon the United States. The execution and filing of the Memorandum of Understanding is a condition precedent for counsel for the defendant or any other person assisting the defense to have access to classified information.

The Classified Information Procedures Act: No motion has been made by the defense for the disclosure of classified information as of this date. The Court may issue additional Protective Orders as needed. Nothing contained in this Order shall be construed as a waiver of any right of the defendant. Procedures for public disclosure of classified information in this case shall be those established by CIPA. The defense shall comply with the requirements of CIPA Section 5 prior to any disclosure of classified information during any proceeding in this case. As set forth in Section 5, the Defense shall not disclose any information known or believed to be classified in connection with any proceeding until notice has been given to Counsel for the Government and until the Government has been afforded a reasonable opportunity to seek a determination pursuant to the procedures set forth in CIPA Section 6, and until the time for the Government to appeal such determination under CIPA Section 7 has expired or any appeal under Section 7 by the Government is decided. Pretrial conferences involving classified information shall be conducted *in camera* in the interest of national security, be attended only by persons with access to classified information and a need to know, and the transcripts of such proceedings shall be maintained under seal

SO ORDERED at Bridgeport, Connecticut, this 16th day of November, 2020.

/s/ Victor A. Bolden
VICTOR A. BOLDEN
UNITED STATES DISTRICT JUDGE